(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 July 2001 (26.07.2001)

PCT

(10) International Publication Number
WO 01/54091 A2

(51) International Patent Classification[7]: G07F 17/00

(21) International Application Number: PCT/US01/01549

(22) International Filing Date: 17 January 2001 (17.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

09/487,651	19 January 2000 (19.01.2000)	US
09/634,034	8 August 2000 (08.08.2000)	US

(71) Applicant: **CYBERLOCATOR, INC.** [US/US]; 2465 Central Avenue, #110, Boulder, CO 80303 (US).

(72) Inventors: **WHITE, William, M.**; 1165 Pennsylvania St., #1A, Denver, CO 80203 (US). **GOLD, Kenneth, L.**; 4500 Ottawa Place, Boulder, CO 80303 (US). **MACDORAN, Peter, F.**; 4225 26th Street, Boulder, CO 80304 (US). **ANDERSON, Steven, M.**; 109 Emerald Street, Broomfield, CO 80020 (US). **COFFEY, Mark, A.**; 1265 Fairfield Drive, Boulder, CO 80303 (US).

(74) Agents: **FOLSOM, Thomas, C.** et al.; Chrisman, Bynum & Johnson, P.C., 1900 Fifteenth Street, Boulder, CO 80302 (US).

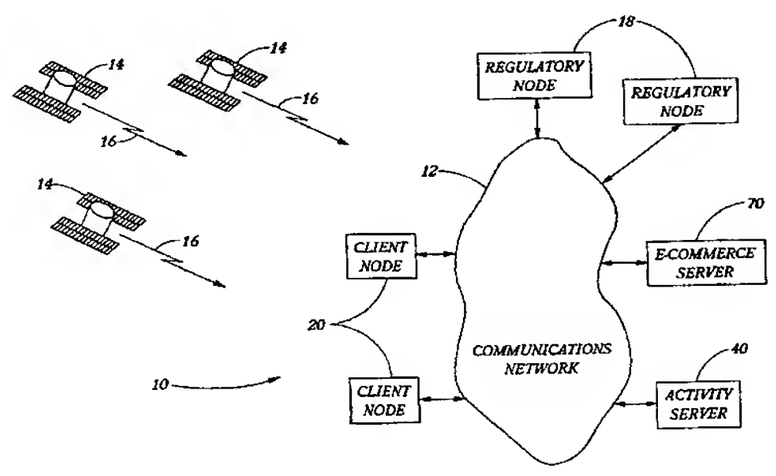
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR CONTROLLING ACCESS TO AND TAXATION OF GAMING AND OTHER ACTIVITIES OVER A COMMUNITATIONS NETWORK



(57) Abstract: A method and system for controlling access to and regulation of access to Internet provided services and goods based on the location of a user's or client's access node. In one implementation, a user location-based control system is provided that includes client nodes, activity servers, such as e-commerce and gaming servers, and regulatory nodes. The process implemented by the control system involves receiving at an activity server a request from a client node for access to the activity. The activity server challenges this access request and determines the location of the client node. In one embodiment, location determination is completed by the client node operating a GPS sensor, a GPS data service, and a locator plugin to create a GPS-based location signature which is transmitted to the activity server. The activity server combines this location signature with its own location signature and then determines the geolocation of the client node. This geolocation is then used by the activity server to approve access based on acceptance criteria including preauthorized locations for client nodes and preauthorized geographical areas or jurisdictions for access. The geolocation is further used by the activity server to look up in a database the appropriate tax jurisdiction and corresponding tax rate for the activity. This tax rate is then applied by the activity server, and the relevant portions of the transaction are stored in memory for transmittal to the appropriate regulatory agency through its access node. Methods for defending against a relay attack are described.

WO 01/54091 A2

Method And System For Controlling Access to And Taxation of Gaming And Other Activities Over a Communications Network

Technical Field

The present invention relates to a computer method and system for controlling, monitoring, and auditing access to and taxation of gaming and other activities over a communications network, such as the Internet, and more particularly to a computer method and system that determines the geolocation of a client node, such as a terminal, computer, or computer network housed in a single building or enclave that is used for accessing the Internet, and then utilizes the determined geolocation to authorize remote access via the communications network to servers and Web sites and other computer devices providing gaming activities or other services (such as electronic commerce) and to control taxation of such remotely accessed activities.

Background Art

The global use of communication networks, especially the Internet, has dramatically increased in recent years and will continue to expand as technological and regulatory problems are overcome. The uses include a wide spectrum of activities from electronic mail to electronic commerce, gaming (e.g., online wagering and the like), and other activities which may require more control over users' access and more regulatory monitoring (e.g., over taxation of such activities). The communications networks are often very large, such as the Internet which is made up of thousands of interconnected networks that cross political borders into hundreds of countries with each network including large numbers of remotely-located client nodes (e.g., any user interface that provides a network connection point, such as a terminal, a computer, a television receiver system configured for WebTV, and the like) and computer networks. "Networking" has until recently been completed with physical telephone lines, cable television wires, and other telecommunication hardware but, more recently, has been achieved with wireless technology, thereby allowing a client node to be completely portable and mobile, such as a cellular phone or other hand-held device. The networked client nodes and computer networks exchange information using various services, such as electronic mail, Gopher, and the World Wide Web. The World Wide Web allows a server computer network or system (e.g., a Web server or Web site) to send Web pages of information to a remote client node or computer network. The information is typically accessed or displayed using a browser or other application program which allows a user to easily understand the shared information at their client node. Similarly, when a user wants to access a Web site or activity, the user requests access by using a browser or other application to transmit the request and to provide additional information (i.e., participate in the activity, such as remote gaming and electronic commerce).

The increase in the number and variety of activities performed over communications networks has brought about a number of problems for the industries operating the activities and the governments

regulating such activities within their borders. For example, operators of certain activities, including gaming, must tightly control users' access to the activities for security reasons and for government regulatory reasons, e.g., an activity may be banned or considered illegal in specific municipalities, states, or countries. Prior to this invention, efforts in the gaming industry have been directed at overcoming technological problems with providing real-time access to a specific gaming activity and security was typically limited to user passwords and encryption methods. For example, see U.S. Patent No. 4,467,424 of Hedges et al., U.S. Patent No. 5,809,482 of Strisower, and U.S. Patent No. 6,001,016 of Walker et al. However, the legality of a user accessing an activity, such as gaming, is typically determined based on the location of the user because that user is generally governed by the laws of the municipality, state, and/or country in which they are presently located. Similarly, government regulation of an activity on a communication network is typically based on the location of the user. For example, the taxation of gaming and electronic commerce activity is generally based on the location of the user, e.g., the user's location determines the municipal, state, and country tax rates applied to the present activity.

Presently, operators of these activities and providers of services, such as electronic commerce, pass the responsibility for complying with laws and regulations onto the user through notices (e.g., "as a user, you accept responsibility for complying with the applicable laws in your governmental jurisdiction" and the notice may list countries where an activity is prohibited) and through disclaimers of responsibility. In other words, the user is made responsible for not accessing activities that are prohibited in their municipality, state, or country and also, for reporting their activities, such as winnings from online gaming and purchases from remote sellers of goods and services, to the appropriate governmental agencies, such as the state and federal revenue services for users located in the United States. Prior to this invention, the concerned governmental agencies and officials had no effective means for monitoring their citizens' uses of communications networks, such as the Internet, and they were unable to monitor access to prohibited activities or to determine, let alone collect, taxes that arose because of such activities.

Consequently, there remains a need for a method and system for meeting the needs of service providers and activity operators and governmental agencies in controlling access to and regulation, including taxation, of gaming and other activities that are accomplished over a communications network, such as the Internet, thereby further legitimizing the provision of these services and activities over a communications network.

Disclosure of Invention

It is an object of the present invention to provide a method and system for monitoring and controlling remote user access to activities provided over a communications network.

It is a related object of the present invention to provide a method and system for monitoring and controlling remote user access to activities provided over a communications network, where such user access authorization is dependent on the location of the user.

It is another object of the present invention to provide a method and system for monitoring and controlling regulatory compliance, such as taxation, of a user remotely accessing activities and services provided over a communications network.

It is a related object of the present invention to provide a method and system for monitoring and controlling regulatory compliance, such as taxation, of a user remotely accessing activities and services provided over a communications network, where such regulations are specific to the location of the user.

Additional objects, advantages, and novel features of the invention will be set forth in part in the description that follows, and in part will become apparent to those skilled in the art upon examination of the following or may be learned by the practice of the invention. The objects and the advantages may be realized and attained by means of the instrumentalities and in combinations particularly pointed out in the appended claims.

To achieve the foregoing and other objects and in accordance with the purposes of the present invention, as embodied and broadly described therein, a user location-based, access control system is provided that generally comprises client nodes, activity servers (e.g., e-commerce servers, gaming servers, and the like), and regulatory nodes or servers all networked together through connections with a communications network. Generally, a user of one of the client nodes requests access to one of the activity servers and shares location information with the activity server as part of obtaining access. The activity server processes this location information along with its own separate location information to determine the location (i.e., geolocation) of the client node. The activity server is further configured to determine if access should be granted to the user based on, among other factors, the location of the client node. If the access is granted, the activity server operates to track the user's session on the activity server and to apply proper taxation to the session based on the transaction within the session and, significantly, upon the location of the client node. The activity server communicates with the regulatory nodes to share information, such as the location of regulatory jurisdiction boundaries, a listing of prohibited activities within the jurisdictions, and taxation rates within each jurisdiction on specific activities.

According to one aspect of the access control system, the geolocation is accurately determined for a client node used by a user to access the communications network. Although a number of methods of locating the client node can be used to practice the invention, a preferred embodiment includes the use of signals from a location-navigation system such as a terrestrial network or a satellite constellation network. In one embodiment, Global Positioning Satellites (GPS) are used to accurately, i.e., within

threshold limits of 100 meters, 5 meters; or even less than 1 meter (i.e., down to a few centimeters), determine the client node geolocation. As will become clear from the following discussion, this level of accuracy is necessary for accurately determining geopolitical borders or governmental jurisdiction boundaries, and this accuracy is obtained in one embodiment of the invention with a differential solution which minimizes risks of "border disputes" over proper positioning of the geopolitical borders or governmental jurisdiction boundaries. To further use of the GPS signals, both the client nodes and the activity servers include sensors for receiving the GPS signals and data service devices for processing the signals. The client node is configured to develop a location signature from the pre-processed GPS signals and to transmit the location signature to the activity server. The activity server receives the client node location signature, combines it with its own location signature developed from its received GPS signals, and then uses all of this information to calculate a differential GPS solution which provides a three-dimensional offset vector which accurately identifies the location of the user's client node relative to the activity server. The location signatures, in this embodiment, are continuously changing everywhere on the Earth and are non-repeating due to the movement of the Earth and the orbiting GPS satellites. Consequently, the location signatures can be used to calculate a location of each specific client node free from concerns about spoofing (i.e., transmission of improperly generated location signatures to provide a false location).

According to a related aspect of the control system, the client node is configured such that the determination of the client node location signature and the transmission of this location signature to the activity server is not seen by, i.e., transparent to, the individual user. This can be achieved in a variety of methods including the use of a browser with a locator plugin as part of the client interface of the client node. The locator plugin comprises software that functions to automatically collect GPS information from the data service device and the sensor during the process of accessing an activity server that requests a location signature to access the server. The locator plugin can also provide the functions of calculating the location signature, date stamping the location signature with information from the client node clock, and transmitting the location signature through the client node communication port to the communications network and to the activity server. In this fashion, the user is not aware, or burdened by, receiving on their browser requests for a location signature and the need for properly instructing the browser and/or client node to obtain and transmit the location signature every time they attempt to access activity servers employing the features of the invention. Of course, this feature of the invention could also be resident or installed on a layer other than the application layer, such as the session layer, the transport layer, or even the packet layer.

According to another aspect of the invention, a method of controlling access to an activity server over a communications network is provided that is based on the location of the user. Due to the variety of regulations in various governmental jurisdictions, it is often desirable to limit access to a

particular activity, such as gaming or the sales of certain products, provided over a communications network based on the geographic location at which a user is attempting to access the communications network (i.e., the Internet or other communications network). For example, certain jurisdictions may prohibit gaming or the purchase or viewing of pornography, and it is useful for a gaming server or an e-commerce server to be able to block access to activities on their servers based on the location of the user. In this regard, the method generally includes a user initiating from a client node a request for access over a communications network to the activity server and the activity server determining the location of the user. To determine the user's location, a locator plugin within the browser of the client node collects GPS data, creates a location signature, and transmits the location signature to the activity server. The activity server receives this location signature, creates its own location signature based on its GPS data, combines the two, time stamped location signatures, and calculates the location of the client node relative to the activity server. The activity server then determines if access can be approved based on information in an authorized location database (that includes locations which have been pre-approved for access, such as legally sanctioned Internet casinos and the like) and/or an authorized jurisdiction database (that includes jurisdictions which do not have bans on the particular activity provided on the activity server). In one embodiment, the information in the authorized jurisdiction database is obtained directly from regulatory agencies over the communications network by communication with regulatory nodes. In this manner, the authorized jurisdiction database can be updated at least periodically to reflect changes in the regulations and laws of the numerous governmental jurisdictions, thereby providing more effective policing of access to each activity server.

According to yet another aspect of the invention, a method of calculating, applying, and monitoring taxation of activities occurring over a communications network is provided. Generally, this method is uniquely effective due in part to the accurate determination of the location of a user who completes transactions over the communications network, which resolves the problem of user anonymity and of relying on a user to provide accurate geographic location information or to even apply and track taxation on their transactions. The method includes providing a user of a client node access to an activity server, such as a gaming or an e-commerce server, and determining the location of the user's client node (as discussed above for controlling access to an activity server). The method further includes monitoring the user's session on the activity server, which may be a gaming session in which the user wins or loses money and/or a commerce session in which the user makes one or more purchase of goods and/or services, to determine a total transaction amount for the session (e.g., total purchase amount or total winnings/losses amount). The method uses the client node location to identify the proper tax jurisdiction and corresponding tax rate on the provided activity. A record is created for the user in a transaction database by the activity server with user information and session information,

including tax jurisdiction, transaction amount, and taxes charged or withheld by the activity provider. The records in this database can be used by the activity provider for proving compliance with the tax regulations and laws of each jurisdiction, and the method may include transmitting, at least periodically, the records to the appropriate regulatory agencies in the numerous jurisdictions via regulatory nodes connected to the communications network. In the above manner, the invention is useful to service providers in determining proper taxation of activities they provide and in allowing effective documentation of the application of tax to their users, thereby further legitimizing the provision of these activities over communications networks and allowing governmental agencies in monitoring and auditing the service providers.

Other features and advantages of the invention will become clear from the following detailed description and drawings of particular embodiments of the user location-based access control system and method and associated combinations and features of the present invention.

Brief Description of the Drawings:

The accompanying drawings, which are incorporated in and form a part of the specification, illustrate the preferred embodiments of the present invention, and together with the descriptions serve to explain the principles of the invention.

In the Drawings:

Figure 1 is a functional schematic diagram of a user location-based, access control system according to the present invention.

Figure 2 is a schematic block diagram of a client node of the access control system of Figure 1.

Figure 3 is a schematic block diagram of the activity server of the access control system of Figure 1.

Figure 4 is a schematic block diagram of the e-commerce server of the access control system of Figure 1.

Figure 5 illustrates an exemplary transaction database for use by the activity server of Figure 3 and the e-commerce server of Figure 4.

Figure 6 is a flow chart illustrating an exemplary process by which a gaming server, such as the activity server of Figure 3, controls access to the gaming server and applies appropriate taxation to a gaming session based on the location of a user's client node.

Figure 7 is a flow chart illustrating an exemplary process by which the e-commerce server of Figure 4 controls user access to the e-commerce server's goods and services and applies appropriate taxation of the user's purchases based on the location of a user's client node.

Figure 8 is a schematic diagram of a protected enclave model illustrating an exemplary environment outside of a gaming or other regulated environment.

Figure 9 is a schematic diagram of a first relay attack upon the model of Figure 8.

Figure 10 is a schematic diagram of a second relay attack upon the model of Figure 8.

Best Mode for Carrying Out the Invention

With the above summary in mind, it may now be helpful in fully understanding the inventive features of the present invention to provide in the following description a thorough and detailed discussion of a number of specific embodiments of the invention. Specifically, the following discussion emphasizes the features of the invention that provide a method and system for user location-based control of access to and regulation of (e.g., taxation of) activities and transactions that occur over a communications network, with the Web server environment of the Internet being selected as an exemplary, but not limiting application, because of its familiarity, its commercial viability, and its global use. The discussion of the invention will progress from a description of the inventive features and components of the system and progress to the embodiments of the control method from a gaming perspective and an e-commerce perspective.

Referring to Figure 1, a user location-based control system 10 is illustrated in an application for controlling transactions and activity over a communications network 12, such as the Internet. The control system 10 includes regulatory nodes 18, client nodes 20, and an exemplary activity server 40 (which may be any activity that can be provided over a communications network, including, for example, gaming), and an exemplary e-commerce server 70, which are each linked, by any of a number of means such as telephone lines, cable television lines, and wireless methods, to the communications network 12. In general, the client nodes 20 are operated by users to submit requests for access over the communications network 12 to the e-commerce server 70 or the activity server 40. The e-commerce and activity servers 70, 40 challenge the requests by requesting information that can be used to determine the geographic location (i.e., geolocation) of the client nodes 20. The client nodes 20 receive and process GPS signals 16 (e.g., spread spectrum microwave signals) from the GPS satellites 14 visible at the client nodes 20 and transmit location signatures (i.e., a digital digest compilation of real time, raw observations of GPS satellites 14). The servers 40, 70 receive the location signatures, collect and process GPS signals 16 to create their own location signatures, and combine the location signatures to determine the locations of the client nodes 20 relative to the servers 40, 70. Access is then granted or denied by the servers 40, 70 based on these determined locations by comparing the locations of the client nodes 20 with various acceptance criteria, such as preauthorized locations and criteria obtained from the regulatory nodes 18, which will be discussed in more detail below. The control system 10 beneficially enables server operators to effectively control and monitor access to the activities and services they provide based on an accurate determination of the geolocation of the user's client node 20.

Each client node 20 is employed by a user or users to obtain access to the communications network 12 and servers 40, 70. In this regard, the client nodes 20 can be any device useful for accessing communications networks, such as the Internet, and include terminals, computers, wireless

communication devices, television receiver systems configured for WebTV and the like. Further, the client nodes 20 may also be a node linking a number of other devices to the communications network 12, such as a server or computer serving as an access node for a local area network or other arrangement of terminals, computers, and other communication devices. This arrangement of devices may be particularly useful for client nodes 20 that are granted ongoing access to servers 40, 70 based on their location. For example, a client node 20 may represent a protected enclave with a known geolocation that is approved for gaming, i.e., an Internet casino, and the geolocation of this Internet casino-type client node 20 can be used as a form of verifiable password for access to the activity server 40, as will become clearer from the following discussion.

Turning to Figure 2, one embodiment of a client node 20 is illustrated for a user to obtain access to the servers 40, 70. The client node 20 comprises a communication port 22 connected to the communication network 12 and in communication with central processing unit (CPU) 24. The client node 20 further includes a client interface 34 that includes a Web browser 36 for allowing a user to view and input information received and transmitted over the communications network 12. A locator plugin 38 for the browser 36 is added to provide many of the functions of the invention in a manner that is transparent to a user. More specifically, the locator plugin 38 automatically responds to requests for location information from a server 40, 70 by collecting GPS information from an included sensor 28 and data service 26, which may be two devices or integrated into a single device. It should be understood at this point that as an alternate to a plugin at the Web browser or application layer, the invention readily lends itself to implementation at each level or layer of a communications network. For example, in the Internet setting, the plugin, code, and the like can be implemented in the session layer, the transport layer, and even the packet layer of Internet protocol. By moving the technology of the invention to lower levels of the communication network, the invention is able to provide additional and enhanced security and/or authentication benefits.

The sensor 28, e.g., a GPS receiver (such as, for an example but not a limitation, a GPS receiver based on the Rockwell Zodiac chipset) and associated hardware or the like, collects raw GPS signals 16 from GPS satellites 14 and transfers it to the data service 26. The data service is a module responsible for programming the sensor 28, collecting and optionally archiving data from the sensor 28, and formatting it into a valid location signature upon request by the locator plugin 38.

In one embodiment, the data service 26 module is further capable of providing status information for the sensor 28, current GPS satellite 14 constellation information, and other relevant information. The locator plugin 38 then further processes, as necessary, the location signature received from the data service 26, date stamps the location signature, and transmits it via the CPU 24 and communication port 22 to the appropriate server 40, 70. The location signature changes every second or less due to the movement of the satellites and the Earth and acts as a dynamic password for the client

node 20. The location signature is configured into packets prior to transmittal to the servers 40, 70. Again, all of these functions occur rapidly, e.g., in less that a few seconds, and without actions being taken or needed by the user.

Figures 3 and 4 illustrate embodiments of the activity server 40, shown as a gaming server to provide a specific example of an activity that is often regulated by governments, and the e-commerce server 70. As with the client nodes 20, the gaming server 40 and the e-commerce server 70 include communication ports 42, 72, CPUs 44, 74, and clocks 50, 80. The gaming server 40 and e-commerce server 70 also include sensors 48, 78 and data service devices 46, 76 for receiving GPS signals 16 from GPS satellites 14 that are visible at the location of the servers 40, 70 and for preparing real time, location signatures for each server 40, 70. Again, these location signatures are time stamped to allow correlation with time stamped location signatures received from client nodes 20.

In contrast to the client nodes 20, the gaming server 40 and the e-commerce server 70 include authentication services 52, 82 for determining the geolocation of the client nodes 20. A number of methods for determining geolocation could be used in the invention, and further, it will be understood that in addition to GPS systems the location data used to obtain the geolocation can readily be obtained from a number of other location/navigation systems including, but not limited to, terrestrial networks (e.g., Long Range Navigation (LORAN-C) and the like) and non-GPS satellite networks (e.g., Global Navigation Satellite System (GLONASS), Wide Area Augmentation System (WAAS), Global Navigation Satellite System (GNSS), and any other navigation-location satellite constellation). In a preferred embodiment, the methodology employed is that disclosed in U.S. Patent No. 4,797,677 of MacDoran et al. and U.S. Patent No. 5,757,916 of MacDoran et al., both of which are incorporated herein by reference thereto. Generally, the authentication services 52, 82 take as input the location signatures from the client nodes 20 and the servers 40, 70 and calculate the differential GPS solutions needed to fix geolocations of the client nodes 20. As will become clear, the determined geolocations of the client nodes 20 are then used by the server interfaces 54, 84 to determine whether access can be granted to the client nodes 20 and if so, to apply the proper governmental regulations to any user activities/transactions based on the geolocation.

Prior to discussing the server interfaces 54, 84 in detail, it may be beneficial to provide a brief description of the geolocation methods taught in the referenced MacDoran et al. patents. Prior to this invention, location-based access control and regulation (e.g., taxation) of Internet activities has been neglected because it was believed to be too difficult to reliably determine the precise location of a network node. In part this concern was based on the fear that users could falsify or IP spoof their locations. Basically, a triangular relationship exists between three locations (i.e., the client the server, and the individual satellites visible simultaneously at the client and the server sites). Each of the existing 27 satellites of the GPS constellation is orbiting the Earth every 12 hours, and the Earth is

rotating about its rotation axis every 24 hours. Thus, two of the three legs of the triangular relationship are continuously changing while the three-dimensional relationship between the sites of a preauthorized client and the server remains static. It is the always changing two legs (actually pseudoranges) between the satellite to client and satellite to server that creates location-specific dynamic passwords or location signatures that are continuously changing, everywhere on the Earth unique and non-repeating. Considering now that as many as 12 satellites may be received by either the client or the server allows the creation of dynamic passwords that are complex and highly secure. This barrier to spoofing of dynamic passwords comes, in part, from the fact that the random solar wind forces on the GPS satellites cause the actual Earth-centered location of the satellites to be unpredictable in real time to the level of accuracy of a few meters and only geolocations within this small radius will be accepted for such a preauthorized site. With somewhat reduced accuracy, any requirement for a common view of satellites between client and server can be eliminated.

Conventionally operating GPS receivers are typically not suitable for location-based authentication purposes because they normally compute latitude, longitude, and height directly from the GPS signals and display these solutions as output. Consequently, a user could report an arbitrary set of coordinates, and it would be difficult to know if the coordinates were actually calculated by a GPS receiver currently at the location represented by the coordinates. In addition, a spoofer could intercept the coordinates transmitted by a legitimate user, and then replay those coordinates in order to gain entry from an unauthorized location.

The data volume of a single sample of the location-specific dynamic passwords is approximately 100 bytes. A typical client transferred dynamic password or location signature is composed of 60 such 100 byte samples (e.g., a total size of 6 kB) in order to gain access at login from a preauthorized site. The server then processes the raw data from the client with a similar set of raw data as measured by the server using its own GPS receiver and independently acquired GPS satellite orbit elements, in a manner known as a fully differential GPS solution. This differential solution yields the relative three-dimensional separation between client and server, which can be thought of as the geolocation of the client.

Referring again to Figures 3 and 4, the gaming server 40 and the e-commerce server 70 each include server interfaces 54 and 84. The server interfaces 54, 84 function to control access to the servers 40, 70 by receiving access requests from client nodes 20, transmitting location signature queries to such client nodes 20, and comparing geolocations determined by the authentication services 52, 82 with a number of acceptance criteria. In the Web server environment, the server interfaces 54, 84 may be Web server hooks, such as Computer Graphics Interfaces (CGIs), that intercept requests for access to the servers 40, 70 and/or to protected data and responds by challenging the potential users with location signature queries and in some embodiments, further information such as user passwords and

user identification numbers/codes which may be combined with the geolocation for further security. The client nodes 20 or potential users respond with location signatures which the servers 40, 70 convert into geolocations, as discussed above.

The server interfaces 54, 74 then compare the geolocation of the client node 20 to one or more acceptance criteria stored in the servers memory or alternatively, within a separate server or memory device (which may be useful if several servers share acceptance criteria databases). In a preferred embodiment, the acceptance criteria are location-based criteria, including, but not limited to, an authorized location which means a client node site that has been preauthorized for access to the server 40, 70 and an authorized jurisdiction which generally includes larger areas, such as all locations within a governmental jurisdiction (e.g., a location within the boundaries of the United States of America or within a specific state). The authorized locations are stored within an authorized location database 56, 86 in each server 40, 70. For servers 40, 70 requiring preauthorization for access, the server interface 54, 84 compares the geolocation with the authorized locations in the databases 56, 86 to determine if access is to be granted. Typically, a predetermined range about the authorized location will be accepted to allow for some error in the determination of the geolocation, and the size of this range will vary with the equipment utilized and with the security required by the server 40, 70 but can be less than a few meters or even less than a few centimeters in some cases. In other cases where access can be granted to any user located in a jurisdiction (e.g., in a jurisdiction where gaming is not prohibited or where purchase of certain products/services is allowed), the server interface 54, 74 determines if the determined geolocation of the client node 20 is within the boundaries of the authorized jurisdictions (e.g., geopolitical borders) in databases 56, 86.

If access is authorized or granted, the server interface 54, 74 tracks the transaction completed by the user from the client node 20 and verifies that proper governmental regulations are complied with during the transaction. These regulations may include a number of requirements of users of the communication network 12, but for ease of description, taxation will be stressed in this description. In this regard, the server interfaces 54, 84 include tax jurisdiction databases 60, 90 that include the boundaries of municipal, state, and federal tax jurisdictions for the services and goods that they provide over the communications network 12. Significantly, the geolocation is used to go into these databases and determine the appropriate tax jurisdiction(s) and tax rate(s) to be applied to the user's transaction. In this manner, proper taxation of the activity does not rely on proper input from the user or upon the user complying with tax regulations after the transaction is completed (e.g., to report Internet purchases).

The information for the transaction is stored in a transaction database 62, 92, for which an exemplary embodiment of a single user's record is illustrated in Figure 5. For each transaction, the server interface 54, 84 stores information, or updates as appropriate, the following fields: the user's

name 102, social security number 104, identification number 106, mailing address 108, authorization status 110, payment card number 112 (e.g., credit or debit card number or account number), transaction total 114, determined tax jurisdiction 116, taxes charged and/or withheld on the transaction 118, and service provider's tax identification number 120. The authorization status 110 field can be used as another acceptance criterion by the server interface 54, 84 by having a status, such as "active," for users who have continuing rights to access the server 40, 70 and "inactive" for users who need to be re-authorized (for failure to pay an invoice, comply with a regulation, and the like). Similarly, the social security number and/or the identification number fields 104, 106 can contain information that can be used by the server interface 54, 84 as another acceptance criterion. The tax jurisdiction 116 field contains information obtained from the tax jurisdiction database 60, 90 and typically will include the tax rate to be applied to the transaction total for each tax jurisdiction. In this manner, the records in the transaction database 62, 92 serve as a complete record of compliance with the regulations of the regulatory jurisdiction wherein the user is operating the client node 20 to access the server 40, 70. These records can then be transmitted, at least periodically, to the appropriate regulatory agencies through standard postal channels or over the communications network 12 to the appropriate regulatory node 18 as verification that the operators of the servers 40, 70 are complying with regulatory agency requirements.

Figure 6 illustrates a user implemented gaming session or process in accordance with the present invention. The gaming session is started and initiated at 122 by the remote user requesting access over a communications network, such as the Internet, to a gaming server (e.g., similar to the server 40 of Figure 3). In one embodiment, the request of 122 is performed by a Web browser on the user's client node. The gaming server then operates at 124 to determine the location, i.e., geolocation, of the user's client node. This determination is typically performed by software and hardware on the gaming server and the browser of the user that functions in combination. The gaming server challenges the user's request by requesting a location signature from the user through their browser. At 126, the user's browser, through a locator plugin, data service, and GPS sensor, collects GPS data and creates a location signature. The client node then transmits the location signature at 128 to the challenging gaming server. At 130, the gaming server determines its own location signature in a similar fashion with GPS data, combines its location signature with the user's client node location signature, and determines the absolute coordinates of the geolocation of the user's client node.

With the geolocation determined in 124, the gaming session proceeds to a step wherein the gaming server approves or denies the user's access at 132 to the gaming server based on the geolocation of the user's client node. This approval step of 132 includes comparing the geolocation with a listing of preauthorized geolocations stored in memory (such as in a database 56 as shown in Figures 3 and 5) in the gaming server or accessible by the gaming server. For example, in gaming

applications, the preauthorized locations may include enclaves or sites that are approved by the gaming operator and/or governmental agencies for remote gaming and can be thought of as "Internet Casinos" and the like. These Internet Casinos may comprise a single computer or a network of computers, terminals, and other electronic devices all housed within a single enclave (e.g., a single building with a client node 20 such as that shown in Figure 2). In this example, user's access will be approved if the geolocation calculated based on the user's client node location signature matches (i.e., within an acceptable geolocation radius or threshold such as less than 100 meters, less than 5 meters, and less than 1 meter down to a few centimeters) the stored geolocation of a preauthorized site. If access is denied because a match is not obtained, the user's session is ended. If access is granted, the gaming session proceeds to 134.

Although not shown, an initial authorization step may be included in this process to allow new users and their client node locations to be registered or added to the authorized location database. This may include requesting the user to transmit a number of location signatures over a certain period of time. The geolocation of the client node can be calculated at each transmission time to "fix" the preauthorized client node location and this fixed geolocation can be added to the authorized location database. This is an effective method of fixing a location without spoofing or falsification because the location signatures are nearly continuously changing with a new location signature being created every second or less.

Alternatively or additionally, the approval step 132 may include comparing the geolocation of the user's client node with a list or map of governmental jurisdictions wherein the gaming activities provided by the gaming server are not prohibited (or conversely, with a list of jurisdictions that prohibit the gaming activity to properly deny the access for any geolocation matches). For example, a single country (or municipality or state within a country) may legalize remote gambling over a communications network. The boundaries of this country are entered into a database or digitally mapped in memory accessible by the gaming server. The information as to which jurisdictions should be included can be obtained directly from the appropriate regulatory agencies of this country. During step 132 of the gaming session, the gaming server compares the user's client node geolocation with these stored boundaries and if the geolocation is within the boundaries, access is approved and the session proceeds to 134.

At 134, the gaming server tracks the user's gaming session by, for example, keeping a record of wager amounts and winnings and losses to obtain final winnings and losses. When wagering and wager results are known, the gaming session continues to 136 where the gaming server updates the user's records to reflect the recent transaction. This may be achieved by updating a transaction database with records for each user and gaming session. This update 136 preferably includes determining the appropriate tax jurisdiction for the user based on their geolocation and a listing or

database of tax jurisdictions. With the tax jurisdiction known, the gaming server applies the appropriate tax rates to the gaming session and records this information in the transaction database. These transaction records are transmitted at 138 to the appropriate regulatory agency or regulatory server/node. Of course, this transmission step 138 can be performed for each transaction or at the rate requested by the regulator agency or not at all if not requested or required by the regulatory agency. The gaming session is then terminated, and this process is repeated each time a user logs in or attempts to access the gaming server over the communications network.

Figure 7 illustrates a user implemented electronic commerce or e-commerce session or process in accordance with the present invention. The e-commerce session is started and initiated at 140 by a remote user requesting access over a communications network to the e-commerce server (such as e-commerce server 70 shown in Figure 4). In this step 140, the user may enter user information to identify themselves, such as the information shown in transactional database 92 (i.e., name, social security number, mailing address, and other) for this e-commerce transaction. The e-commerce server at 142 stores this information in appropriate fields in a transaction database and grants initial access to the Web site(s) available through the e-commerce server. The user is then allowed to freely navigate with their browser the e-commerce Web site(s) and indicate intended purchases at 144. If access to the Web site would be restricted by certain jurisdictions (such as for a site that allows access to banned or restricted audio or visual works), the determination of whether the user is to have access can be moved to an earlier position in the e-commerce process (i.e., no "initial access" would be granted).

With the intended purchases and total pretax transaction amount known, the e-commerce session proceeds to 146 in which the e-commerce server determines the location of the user's access or client node. As with the gaming session discussed above, a number of methods can be used to determine the location of the user's client node in step 146. As illustrated, this location step 146 includes the e-commerce server challenging the client node to have a locator plugin on the user's client node browser collect GPS data and use this GPS data to create a location signature for the client node at 148. The client node then transmits this location signature to the e-commerce server at 150. At 152, the e-commerce server determines its own location signature with time stamped GPS data, combines the two location signatures, and calculates the absolute coordinates of the geolocation of the user's client node. In this manner, the location of the user's client node is accurately determined by the e-commerce server at 146.

The e-commerce server may offer goods and services that are regulated or prohibited in certain governmental jurisdictions. In this regard, the user's purchases can be approved based on the geolocation of the user's client node at 154 by comparing the geolocation with authorized locations stored in an authorized location database and/or with authorized jurisdictions stored in an authorized jurisdiction database. As a specific example, it may be illegal to purchase World War II artifacts in

Germany. If an operator of an e-commerce server sells these artifacts, the operator can in step 154 deny access to any users who access their e-commerce server from Germany by comparing the client node geolocation with the authorized jurisdiction database (as stated above, depending on the goods and services provided, it may be easier for the operator to track jurisdictions that prohibit the purchase of the goods and services rather than the jurisdictions that allow these purchases). If access is not approved, the user's session is ended prior to completing the purchasing transaction. If access is approved, the e-commerce session continues to step 156.

In step 156, the e-commerce server updates the transaction records for this user and this transaction. This step 156 preferably includes determining the user's tax jurisdiction and appropriate tax rates for the purchases based on the geolocation that are used to access a tax jurisdiction database that includes tax jurisdiction boundaries and tax rates for various purchases of goods and services (e.g., tax rates for the goods and services provided by the e-commerce server operator). The tax rate is applied to the transaction amount (or amounts, if there is more than one applicable tax rate) and the tax charged is recorded in the transaction records and/or transaction database. The transaction records are transmitted at 158 directly to the regulatory agencies through its access nodes, and as with the gaming session discussed above, this step is optional and depends upon the requirements of the regulatory agency. After step 158, the e-commerce session is ended, with the e-commerce operator retaining a complete record of the transaction.

Additional Security Features and Configurations to Protect Against Relay Attacks

As previously discussed above, in connection with Figures 3 and 4 and elsewhere, an illustrative embodiment of the activity server 40, was shown as a gaming server to provide a specific example of an activity that is often regulated by governments. In a preferred embodiment, the methodology employed is that disclosed in U.S. Patent No. 4,797,677 of MacDoran et al. and U.S. Patent No. 5,757,916 of MacDoran et al., both of which have already been incorporated herein by reference thereto. A brief description of the geolocation methods taught in the referenced MacDoran et al. patents has already been provided. In summary, prior to this invention, location-based access control and regulation (e.g., taxation) of Internet activities has been neglected because it was believed to be too difficult to reliably determine the precise location of a network node. In part this concern was based on the fear that users could falsify or IP spoof their locations. Basically, a triangular relationship exists between three locations (i.e., the client, the server, and the individual satellites visible simultaneously at the client and the server sites). Each of the existing 27 satellites of the GPS constellation is orbiting the Earth every 12 hours, and the Earth is rotating about its rotation axis every 24 hours. Thus, two of the three legs of the triangular relationship are continuously changing while the three-dimensional relationship between the sites of a preauthorized client and the server remains static. It is the always changing two legs (actually pseudoranges) between the satellite to client and satellite to

server that creates location-specific dynamic passwords or location signatures that are continuously changing, everywhere on the Earth unique and non-repeating. Considering now that as many as 12 satellites may be received by either the client or the server allows the creation of dynamic passwords that are complex and highly secure. This barrier to spoofing of dynamic passwords comes, in part, from the fact that the random solar wind forces on the GPS satellites cause the actual Earth-centered location of the satellites to be unpredictable in real time to the level of accuracy of a few meters and only geolocations within this small radius will be accepted for such a preauthorized site. With somewhat reduced accuracy, any requirement for a common view of satellites between client and server can be eliminated. Conventionally operating GPS receivers are typically not suitable for location-based authentication purposes because they normally compute latitude, longitude, and height directly from the GPS signals and display these solutions as output. Consequently, a user could report an arbitrary set of coordinates, and it would be difficult to know if the coordinates were actually calculated by a GPS receiver currently at the location represented by the coordinates. In addition, a spoofer could intercept the coordinates transmitted by a legitimate user, and then replay those coordinates in order to gain entry from an unauthorized location.

In accordance with the methods of the referenced MacDoran et al. patents (and as used in this invention), the data volume of a single sample of the location-specific dynamic passwords is approximately 100 bytes. A typical client transferred dynamic password or location signature is composed of 60 such 100 byte samples (e.g., a total size of 6 kB) in order to gain access at login from a preauthorized site. The server then processes the raw data from the client with a similar set of raw data as measured by the server using its own GPS receiver and independently acquired GPS satellite orbit elements, in a manner known as a fully differential GPS solution. This differential solution yields the relative three-dimensional separation between client and server, which can be thought of as the geolocation of the client.

With the foregoing summary in mind, it should be appreciated that the geolocation methods taught in the referenced MacDoran et al. patents may be thought to rely on the concept of the "protected enclave" to ensure that users (that is, any client node) of the system had a vested interest in protecting their premises and, as a result, also an interest in protecting the integrity of the system components. That is, a preferred embodiment of the referenced patents was in the context of computer network security by geolocation, and the client was intent upon protecting the security of its premises (nodes) and the system itself. A schematic diagram of a protected enclave model of a type readily contemplated by the prior MacDoran et al. patents is shown in Figure 8.

With the gaming and similar applications of various embodiment of the instant invention, certain of the assumptions of the model of Figure 8 no longer apply. In particular, the client can not always be assumed to be a protected enclave in the sense that the client has any interest in protecting its

site or in preventing others from abusing the trust structure of the computer network security application shown in the model of Figure 8, or in the prior MacDoran et al. patents. In other words, the location system, as applied in a gaming or other regulated environment pursuant to the present invention must not only be able to authenticate a trustworthy client, but must also be able to authenticate a potentially adversarial client.

A category of attacks on this system may be referred to as "relay attacks". These may consist of setting up an automated PC and GPS device in a valid jurisdiction such that the PC is capable of relaying commands (such as betting information) from a remote site to the local PC, thus making the remote user look like his/her bets are being placed in a legal jurisdiction. A schematic diagram of a first relay attack is shown in Figure 9.

A good example of a potential implementation of this type of relay attack could involve the use of a software program that can reproduce the computing environment of a PC at a remote site. A commercially available product known as PC ANYWHERE might be able reproduce the computing environment at a remote site, and other programs may be available or may be developed to accomplish the same result. Using such a program, a remote client could also initiate a delayed relay attack in which the remote client issues wagering commands to be executed in the near future by the legal client, and then disconnects the relayed channel.

Another potential type of relay attack might involve relaying the information coming out of the authenticated device to a remote site (as shown in the schematic of Figure 10), in effect creating a virtual device at the remote site and enabling a user outside the valid jurisdiction to appear as though they are in the jurisdiction. This can be done by replicating the traffic on the bus (serial, USB, or other) which connects the GPS device to the host PC.

The inventors have explored several defenses to these potential attacks. Possible solutions are listed below along with discussion of certain advantages of each:

1. Administrative limits. This potential defense would limit all user (client) accounts to a single user and would track activity.

Advantages: it is expected that this potential solution would be relatively inexpensive to configure and could be expected to prevent the one-to-many relay attack, similar to what an illegal bookie might use.

2. Biometrics. This potential defense would integrate additional security technologies such as a fingerprint reader, voice recognition, retina scan or other biometric into the device.

Advantages: this would be expected to be the most reliable and non-defeatable way to guarantee that a specific authorized person is present at the device, thereby adding an additional level of security.

3. Card Readers. This potential defense would integrate a swipe card reader, and might require credit card use or other PIN (personal identification number) - type input.

Advantages: it is expected that this potential solution would require human interaction and would possibly require a user to provide account and possibly personal identity or (PIN type) information to the system, thereby adding an additional level of security.

4. Human feedback. This potential defense would require a user to press a button, keypad, or other switch on the authenticated device to get a valid location signature.

Advantages: it is expected that this potential solution would be relatively cheap, and relatively easy to integrate.

5. Tamper-proof device. This potential defense would provide for special ant-tamper (or self-destruct) construction of the authentication device. The device could, for example, be epoxied together or otherwise manufactured so that users cannot take it apart or probe it without destroying it.

Advantages: it is expected that this potential solution would prevent hackers from learning internal workings of the device and then rewiring the device for automatic relay.

6. Digitally signed output. This potential defense would attach PKI public/private keys to all devices and sign the resulting data.

Advantages: it is expected that this solution would use proven crytographic means of establishing authentication of device and message.

7. Time Delay Of Arrival sensing. This potential defense would enable the software in the host computer to use time delay of arrival for messages to and from the authentication device

Advantages: it is expected that this potential solution provides a software method of ensuring that a very long channel (cable, telephone link or RF link) has not been inserted into the bus between the authentication device and the host (client) PC.

8. Open port monitor. This potential defense would enable the software in the host computer to deny location signal access if any non-authorized network connections have been made.

Advantages: it is expected that this potential solution provides a software method of shutting down relay programs and network connections that may be relaying information to/from the host (client) PC.

Since numerous modifications and combinations of the above method and embodiments will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and processes shown and described above. For example, only a limited number of client nodes, regulatory nodes, and activity servers (i.e., an e-commerce and a gaming server) are illustrated and discussed in detail for ease and clarity of description, but it should be understood that any number of nodes and servers can be interconnected according to the invention. Additionally, the type of activity the server provides is not limited to e-commerce and gaming but may be any type of activity that can be

offered over a communications network for which governmental regulation may be desirable and/or for which user location-based access control may be useful.

Further, it should be understood that certain features of the invention could be shared by several client nodes and servers. For example, a single authentication service could be placed on a server accessed by numerous servers, the databases could be placed on a shared server for access by a number of activity/e-commerce servers, and similarly, numerous client nodes could share a single data service module. Similarly, a "client node" could also become a peer node which is another activity server, and in this case, the client node may include some of the features of the servers discussed above (e.g., an authentication service, a server interface with appropriate databases or at least access to such databases). The use of location signatures was discussed in the context of a specific technology for determining geolocations, but the concepts of the invention can readily be applied to other geolocation determining technologies that currently exist or that may be developed in the future.

Accordingly, resort may be made to all suitable modifications and equivalents that fall within the scope of the invention as defined by the claims which follow. The words "comprise", "comprises", "comprising", "include(s)", and "including", when used in this specification and in the following claims are intended to specify the presence of stated features or steps, but they do not preclude the presence or addition of one or more other features, steps, or groups thereof.

Claims:

The embodiments of the invention in which an exclusive property or privilege is claimed which follow:

1. A method of controlling access to and regulation of user access to activities provided over a communications network, comprising:

connecting a server device to the communications network;

providing an activity with said server device over the communications network to users who request access and are granted access by said server device;

from a user's client node, receiving with said server a request for access to said activity provided by said server device;

determining a geolocation of said user's client node; and

granting said user access to said activity on said server device based on said determined geolocation of said user's client node.

2. The method of claim 1, wherein said granting is completed if said determined geolocation is within a set of acceptance criteria.

3. The method of claim 2, wherein acceptance criteria include authorized locations for accessing said server device.

4. The method of claim 3, wherein said granting is completed when said determined geographic location is within a predetermined threshold distance from one of said authorized locations for accessing said server device.

5. The method of claim 4, wherein said threshold distance is less than 100 meters.

6. The method of claim 5, wherein said threshold distance is less than 5 meters.

7. The method of claim 6, wherein said threshold distance is less than 1 meter.

8. The method of claim 2, wherein said acceptance criteria include authorized jurisdictions for accessing said server device defined by geographic boundaries.

9. The method of claim 1, further including after said granting of access, tracking said user's access to said activity to determine a transaction total amount.

10. The method of claim 8, further including using said geolocation to determine a tax jurisdiction and a tax rate for said user, and calculating a tax amount for said user's access based on said tax rate and said transaction total amount.

11. The method of claim 1, wherein said determining includes receiving from said user's client node a location signature based on location data receivable at said client node, simultaneously creating a server device location signature based on location data receivable at said server device, and combining said location signatures to obtain said geolocation of said user's client node.

12. The method of claim 11, wherein said location data is received at said client node from a location-navigation system selected from the group consisting of a terrestrial location-network, a Global Navigation Satellite System (GLONASS), a Global Positioning System (GPS, a Wide Area Augmentation System (WAAS), and a Global Navigation Satellite System (GNSS).

13. The method of claim 1, wherein said activity is gaming or electronic commerce.

14. A method for managing access to goods and services offered by a provider to users over the Internet, comprising:

providing a Web site server connected to the Internet and selectively accessible by users of client nodes connected to the Internet;

receiving from one of said client nodes a Web site access request at said Web site server;

selecting, in response to said Web site access request, to grant or to deny said client node access to a goods and services provider's Web site provided on said Web site server, said selecting including determining a location of said client node relative to a location of said Web site server; and

for client nodes granted access in said selecting, monitoring an Internet session on said Web site to determine and record a total transaction amount based on selection of goods and services for said Internet session.

15. The method of claim 14, further searching a tax jurisdiction database with said location of said client node to identify a tax jurisdiction and a corresponding tax rate for said Internet session.

16. The method of claim 15, further including applying said tax rate to said total transaction amount to determine a tax amount for said Internet session.

17. The method of claim 16, further including communicating a transaction record including said total transaction amount, said tax jurisdiction, said tax amount, and an identification number for said goods and services provider to a regulatory agency monitoring said tax jurisdiction.

18. The method of claim 14, wherein said selecting includes using said location of said client node to search an authorized location database to determine if said location of said client node is an authorized location for accessing said goods and services provider's Web site.

19. The method of claim 14, wherein said selecting includes using said location of said client node to search an authorized jurisdiction database to determine if said location of said client node is within an authorized jurisdiction for accessing said goods and services provider's Web site.

20. The method of claim 14, wherein said determining said location of said client node is calculated from the combination of a location signature of said client node created from location data received at said client node and a location signature of said Web site server created from location data received at said Web site server.

21. The method of claim 20, wherein said location data is received at said client node from a location-navigation system selected from the group consisting of a terrestrial location-network, a Global Navigation Satellite System (GLONASS), a Global Positioning System (GPS, a Wide Area Augmentation System (WAAS), and a Global Navigation Satellite System (GNSS)

22. A user location-based system for managing activities provided on a communications network, comprising:

an activity server in communication with the communications network for selectively providing access to and regulating use of an activity by a user of the communications network;

a client node in communication with the communications network, wherein said client node is operable by a user to transmit an access to said activity server to participate in said activity provided by said activity server; and

means for determining a geolocation of said client node;

wherein said selective provision of access and regulation of use of said activity by said activity server is based on said geolocation of said client node.

23. The system of claim 22, wherein said determining means includes a GPS sensor and a data service device at said client node for receiving and processing GPS signals visible at said client node into a client node location signature and a GPS sensor and a data service device at said activity server for receiving and processing GPS signals visible at said activity server into an activity server location signature.

24. The system of claim 23, wherein said client node includes a communications network browser with a locator plugin for receiving requests for client node location signatures from activity servers and, in response, collecting said client node location signature from said data service and transmitting said client node location signature to said activity server.

25. The system of claim 23, wherein said determining means further includes an authentication service device configured to combine said client node location signature and said activity server location signature to calculate a geolocation of said client node.

26. The system of claim 25, wherein said activity server includes an authorized location database and means for searching said authorized location database with said geolocation for an authorized location within a predetermined threshold range.

27. The system of claim 25, wherein said activity server includes an authorized jurisdiction database and means for searching said authorized jurisdiction database to determine whether said geolocation is within an authorized jurisdiction stored in said authorized jurisdiction database.

28. The system of claim 25, wherein said activity server includes a tax jurisdiction database containing the geographic boundaries of tax jurisdictions and tax rates of said tax jurisdictions

and said activity server further includes a means for using said geolocation to identify said tax jurisdictions and said tax rates that apply to user's access of said activity.

29. The system of claim 28, wherein said activity server further includes a transaction database for storing information including user information, said identified tax jurisdictions, said identified tax rates, a total transaction amount, and a tax charged amount and wherein said activity server includes a means for updating said stored information for each of said accesses of said activity by said user.

30. The system of claim 22, wherein said activity provided by said activity server is gaming or electronic commerce.

31. The method of claims 1 or 14, further comprising the step of protecting the determined geolocation against deception during at least one of the therein named steps.

32. The method of claim 31, wherein the step of protecting the determined geolocation includes using at least one protection technique selected from the group of protection techniques consisting of administrative limits, biometrics, card readers, human feedback, tamper-proof devices, digitally signed output, time delay of arrival sensing, and open port monitoring.

33. The system of claim 22, further comprising an additional security system.

34. The system of claim 33, wherein the additional security system includes at least one security feature selected from the group of security features consisting of administrative limits, biometrics, card readers, human feedback, tamper-proof devices, digitally signed output, time delay of arrival sensing, and open port monitoring.

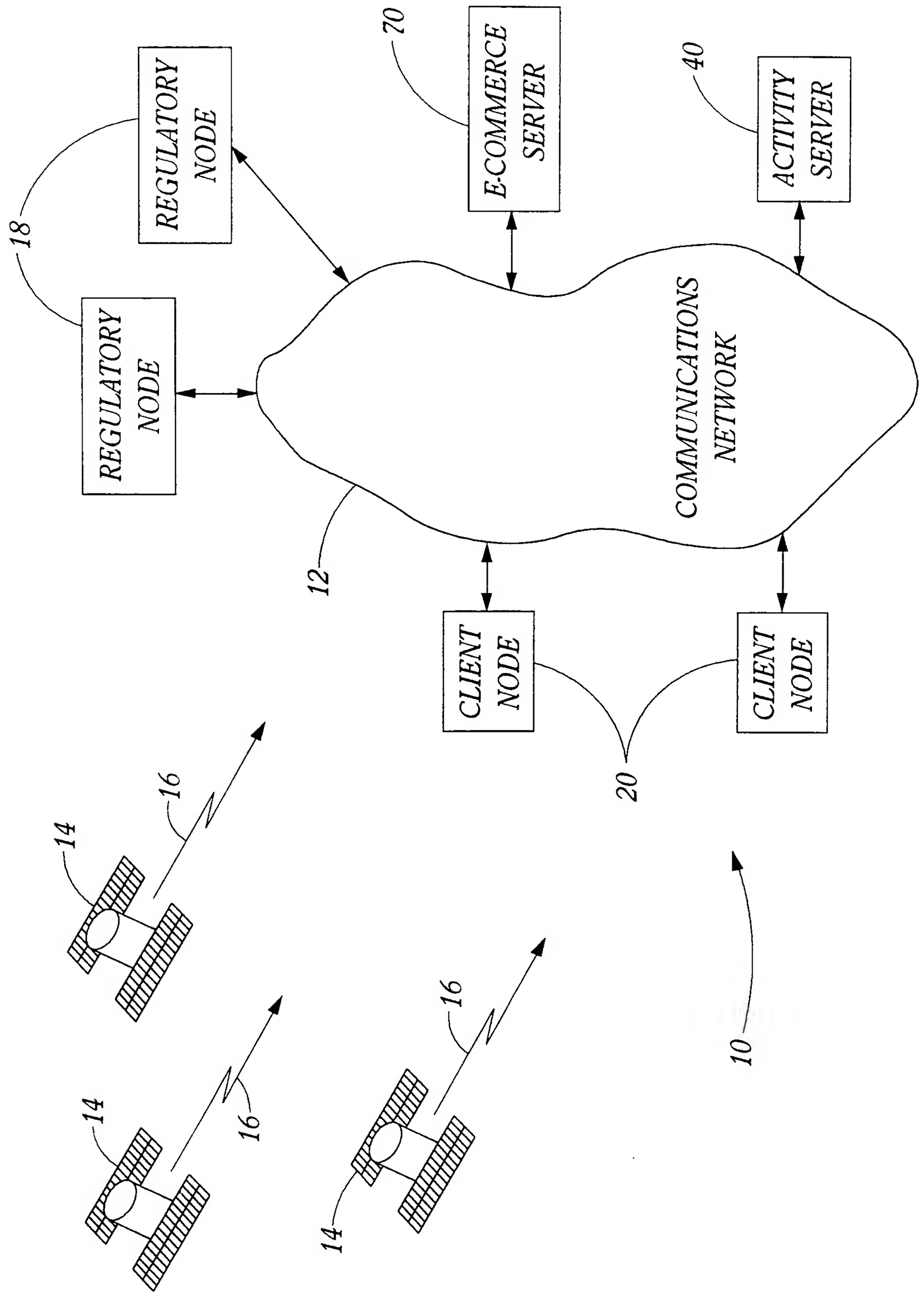

REGULATORY NODE
18
REGULATORY NODE
E-COMMERCE SERVER
70
ACTIVITY SERVER
40
COMMUNICATIONS NETWORK
12
CLIENT NODE
CLIENT NODE
20
14
16
14
16
14
16
10

Figure 1

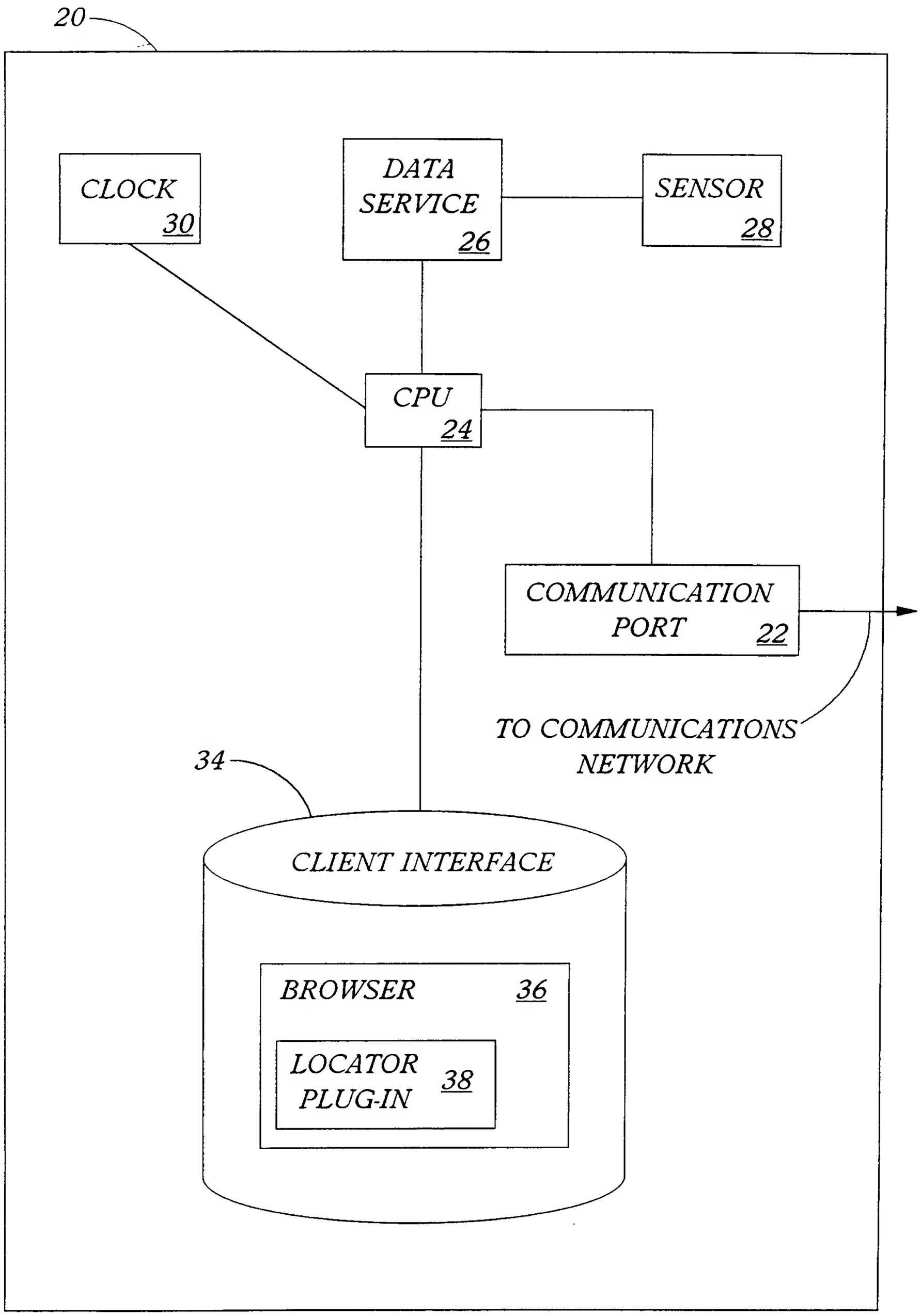

20
CLOCK
30
DATA
SERVICE
26
SENSOR
28
CPU
24
COMMUNICATION
PORT
22
TO COMMUNICATIONS
NETWORK
34
CLIENT INTERFACE
BROWSER
36
LOCATOR
PLUG-IN
38

Figure 2

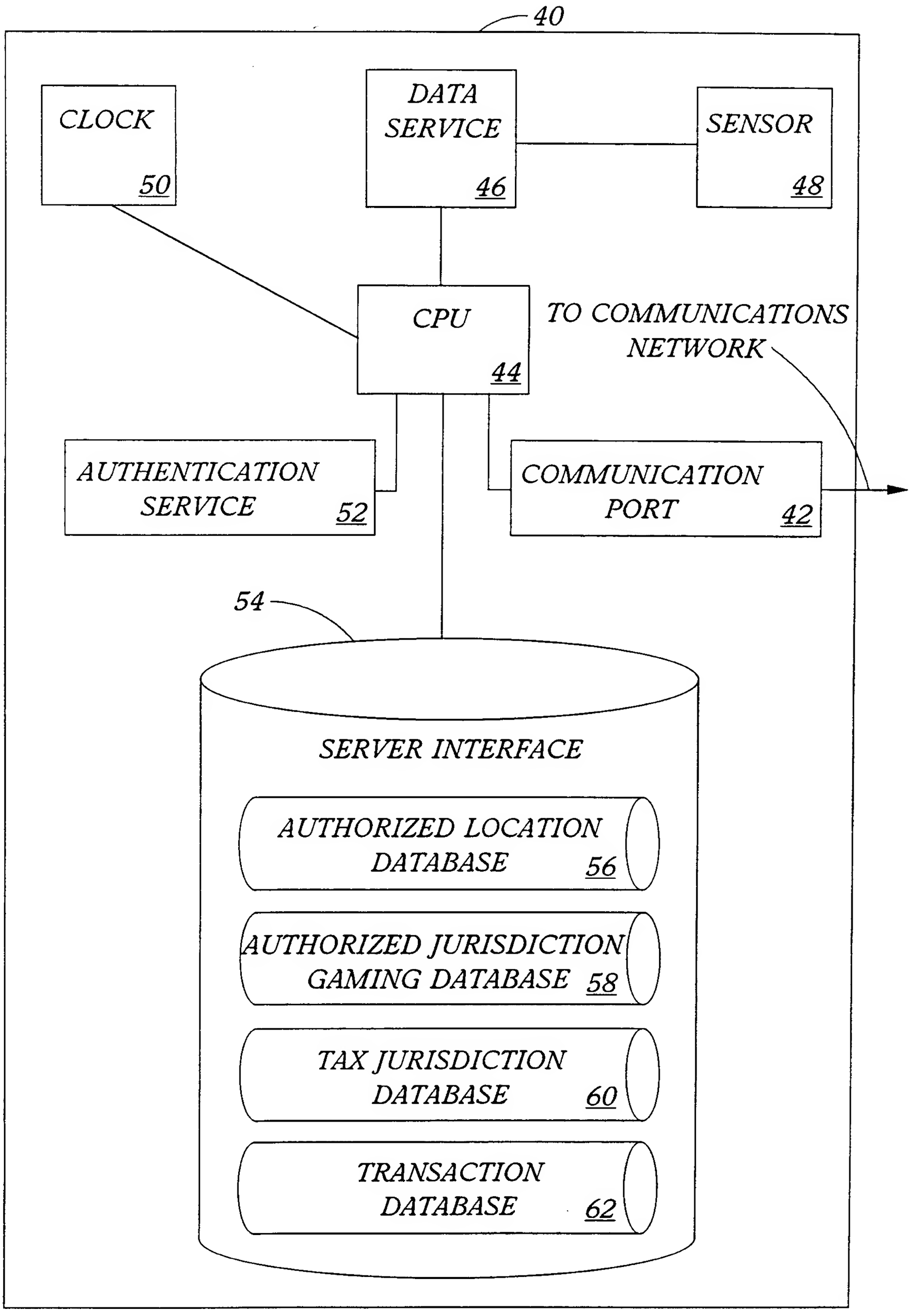

40
CLOCK
50
DATA SERVICE
46
SENSOR
48
CPU
44
TO COMMUNICATIONS NETWORK
AUTHENTICATION SERVICE
52
COMMUNICATION PORT
42
54
SERVER INTERFACE
AUTHORIZED LOCATION DATABASE
56
AUTHORIZED JURISDICTION GAMING DATABASE
58
TAX JURISDICTION DATABASE
60
TRANSACTION DATABASE
62

Figure 3

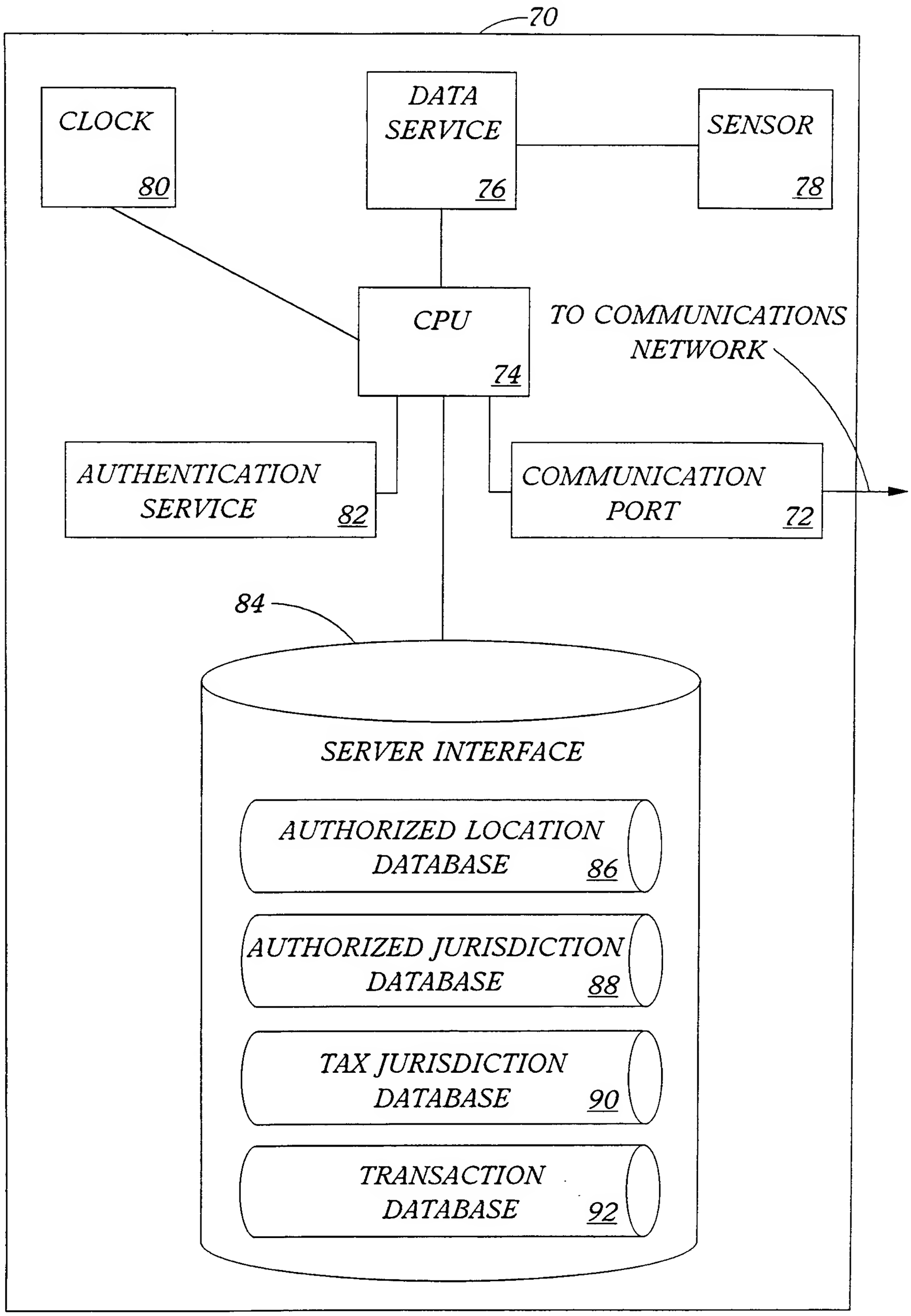

70
CLOCK
80
DATA SERVICE
76
SENSOR
78
CPU
74
TO COMMUNICATIONS NETWORK
AUTHENTICATION SERVICE
82
COMMUNICATION PORT
72
84
SERVER INTERFACE
AUTHORIZED LOCATION DATABASE
86
AUTHORIZED JURISDICTION DATABASE
88
TAX JURISDICTION DATABASE
90
TRANSACTION DATABASE
92

Figure 4

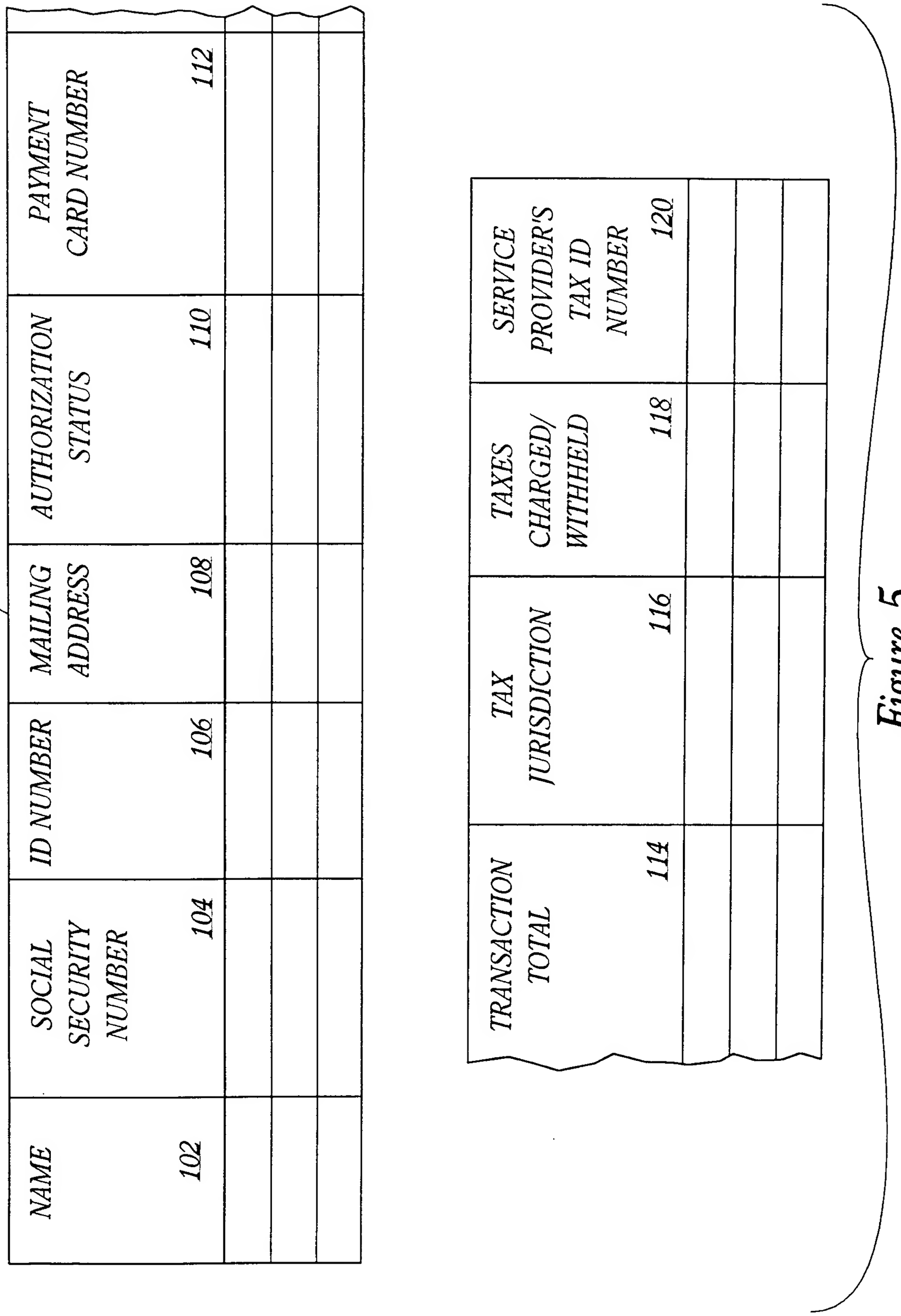

62,92
NAME
102
SOCIAL SECURITY NUMBER
104
ID NUMBER
106
MAILING ADDRESS
108
AUTHORIZATION STATUS
110
PAYMENT CARD NUMBER
112
TRANSACTION TOTAL
114
TAX JURISDICTION
116
TAXES CHARGED/ WITHHELD
118
SERVICE PROVIDER'S TAX ID NUMBER
120

Figure 5

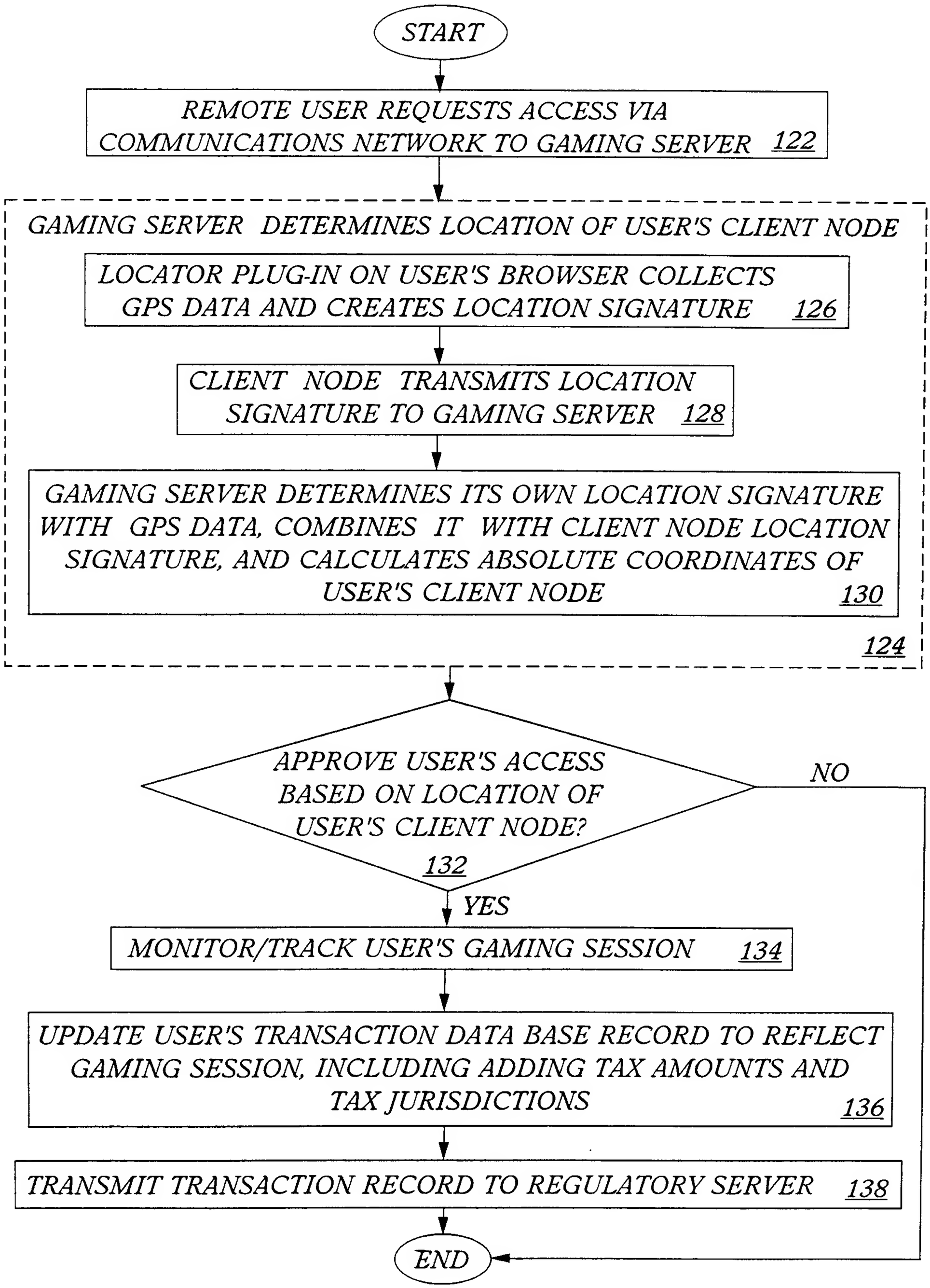

START
REMOTE USER REQUESTS ACCESS VIA COMMUNICATIONS NETWORK TO GAMING SERVER 122
GAMING SERVER DETERMINES LOCATION OF USER'S CLIENT NODE
LOCATOR PLUG-IN ON USER'S BROWSER COLLECTS GPS DATA AND CREATES LOCATION SIGNATURE 126
CLIENT NODE TRANSMITS LOCATION SIGNATURE TO GAMING SERVER 128
GAMING SERVER DETERMINES ITS OWN LOCATION SIGNATURE WITH GPS DATA, COMBINES IT WITH CLIENT NODE LOCATION SIGNATURE, AND CALCULATES ABSOLUTE COORDINATES OF USER'S CLIENT NODE 130
124
APPROVE USER'S ACCESS BASED ON LOCATION OF USER'S CLIENT NODE? 132
NO
YES
MONITOR/TRACK USER'S GAMING SESSION 134
UPDATE USER'S TRANSACTION DATA BASE RECORD TO REFLECT GAMING SESSION, INCLUDING ADDING TAX AMOUNTS AND TAX JURISDICTIONS 136
TRANSMIT TRANSACTION RECORD TO REGULATORY SERVER 138
END

Figure 6

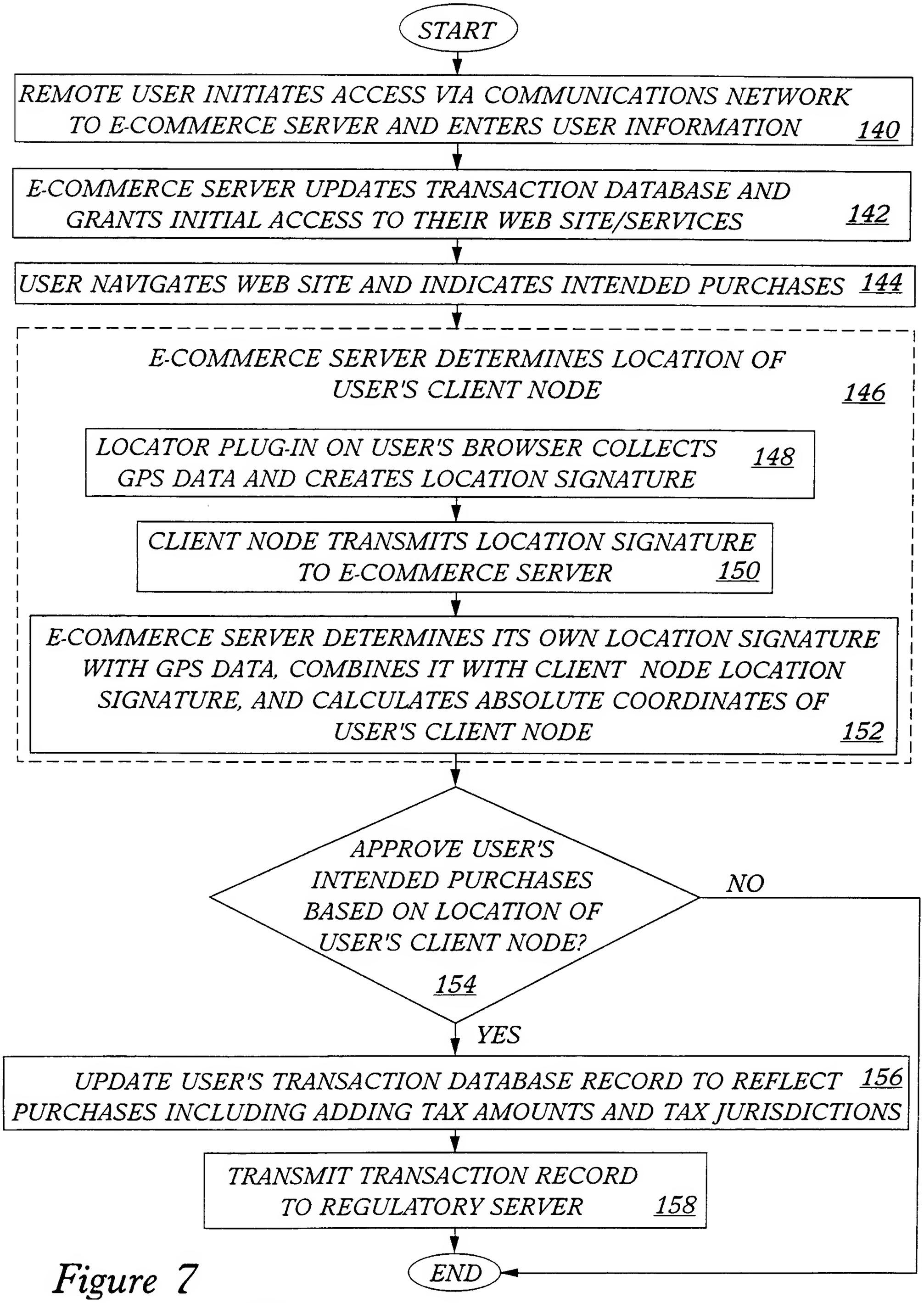

START
REMOTE USER INITIATES ACCESS VIA COMMUNICATIONS NETWORK TO E-COMMERCE SERVER AND ENTERS USER INFORMATION 140
E-COMMERCE SERVER UPDATES TRANSACTION DATABASE AND GRANTS INITIAL ACCESS TO THEIR WEB SITE/SERVICES 142
USER NAVIGATES WEB SITE AND INDICATES INTENDED PURCHASES 144
E-COMMERCE SERVER DETERMINES LOCATION OF USER'S CLIENT NODE 146
LOCATOR PLUG-IN ON USER'S BROWSER COLLECTS GPS DATA AND CREATES LOCATION SIGNATURE 148
CLIENT NODE TRANSMITS LOCATION SIGNATURE TO E-COMMERCE SERVER 150
E-COMMERCE SERVER DETERMINES ITS OWN LOCATION SIGNATURE WITH GPS DATA, COMBINES IT WITH CLIENT NODE LOCATION SIGNATURE, AND CALCULATES ABSOLUTE COORDINATES OF USER'S CLIENT NODE 152
APPROVE USER'S INTENDED PURCHASES BASED ON LOCATION OF USER'S CLIENT NODE? 154
NO
YES
UPDATE USER'S TRANSACTION DATABASE RECORD TO REFLECT PURCHASES INCLUDING ADDING TAX AMOUNTS AND TAX JURISDICTIONS 156
TRANSMIT TRANSACTION RECORD TO REGULATORY SERVER 158
END

Figure 7

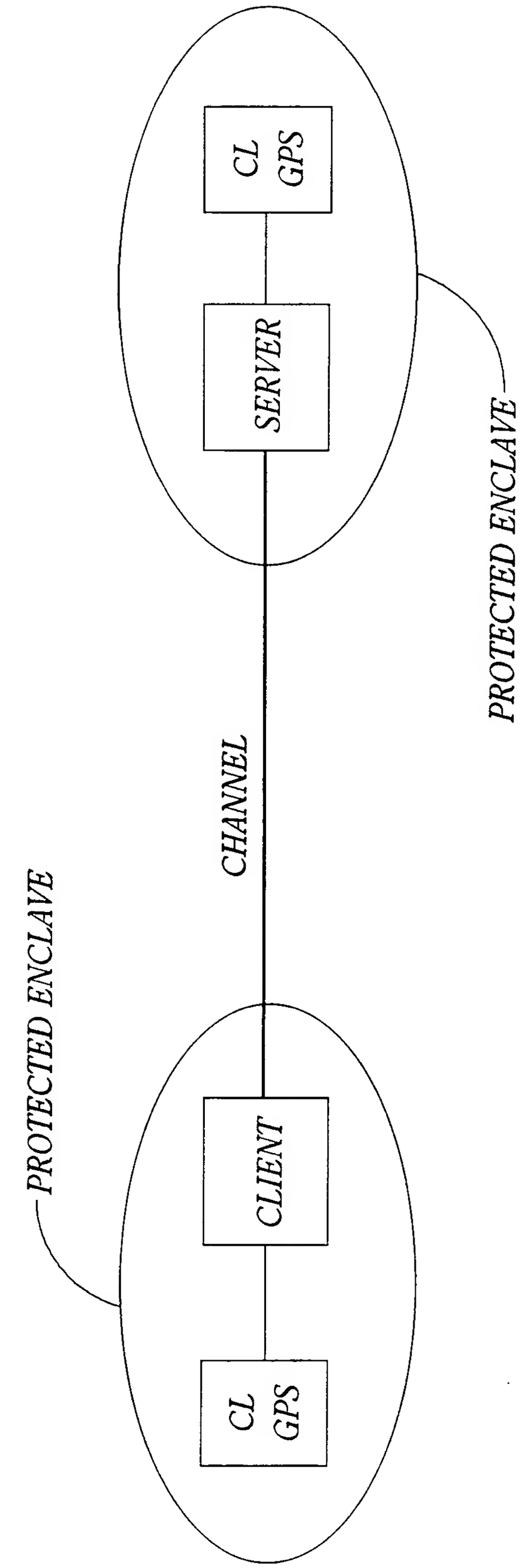

CL
GPS
SERVER
CHANNEL
CLIENT
CL
GPS
PROTECTED ENCLAVE
PROTECTED ENCLAVE

Figure 8

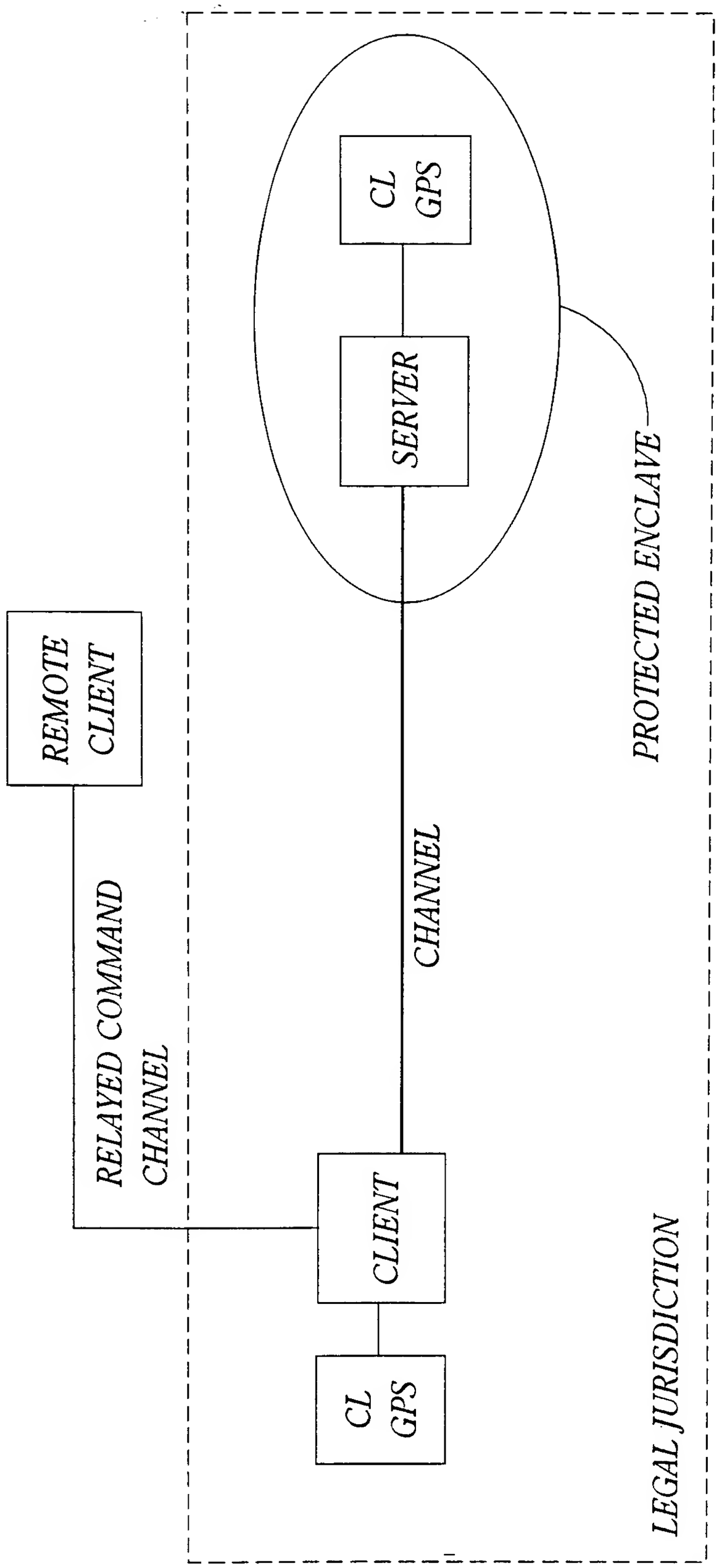

REMOTE CONTROL RELAY ATTACK
PROTECTED ENCLAVE
LEGAL JURISDICTION
CL
GPS
SERVER
CHANNEL
REMOTE
CLIENT
RELAYED COMMAND
CHANNEL
CLIENT
CL
GPS

Figure 9

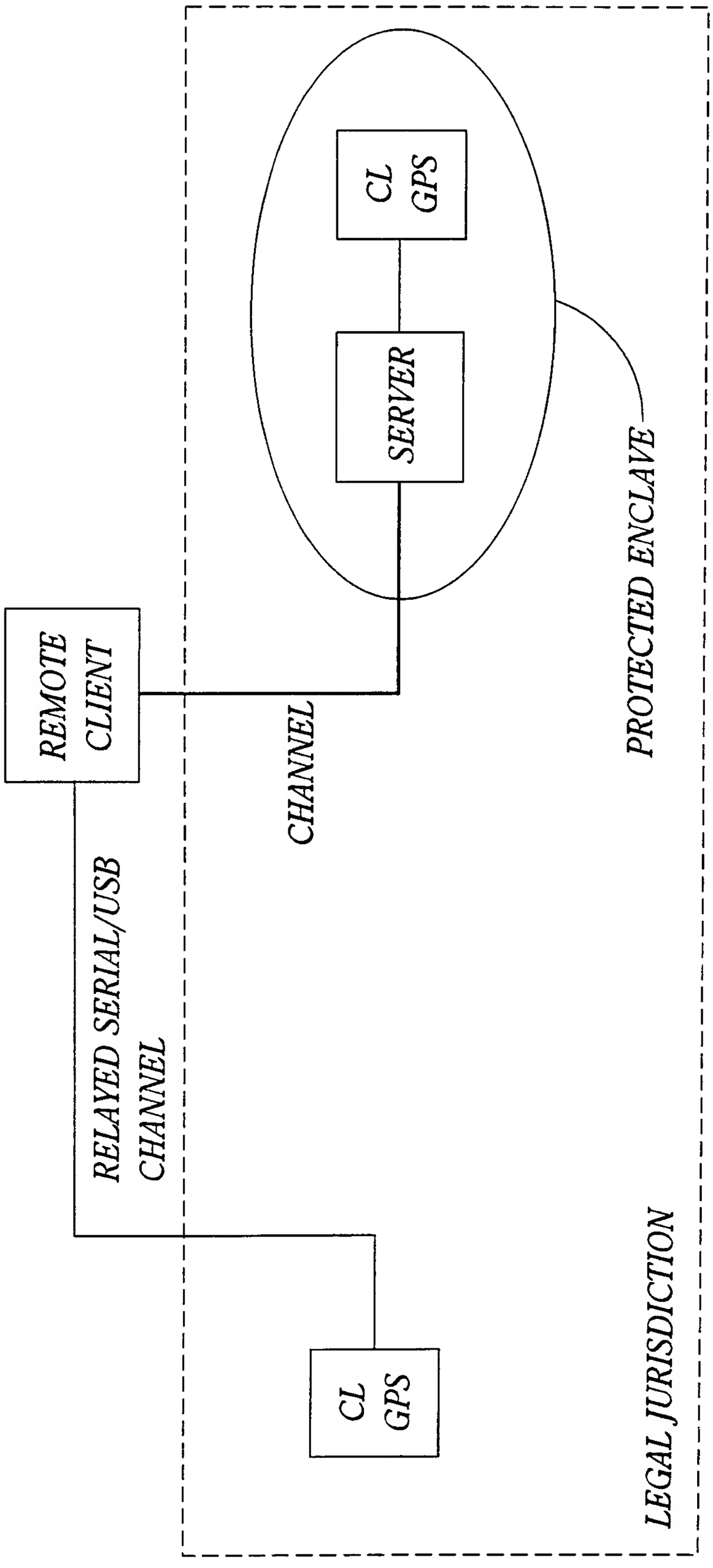

CL
GPS
SERVER
REMOTE
CLIENT
CHANNEL
PROTECTED ENCLAVE
VIRTUAL GPS DEVICE RELAY ATTACK
RELAYED SERIAL/USB
CHANNEL
CL
GPS
LEGAL JURISDICTION

Figure 10